MNE7 Access to the Global Commons
Outcome 3 Cyber Domain

Objective 3.5 Cyber Situational Awareness

Concept of Employment for Cyber Situational Awareness Within the Global Commons

Version 1.0

Dated 25 Feb 2013

Distribution Statement

This document was developed and written by the contributing nations and organizations of the Multinational Experiment (MNE) 7. It does not necessarily reflect the views or opinions of any single nation or organization, but is intended as a guide. Reproduction of this document and unlimited distribution of copies is authorized for personal and non-commercial use only, provided that all copies retain the author attribution as specified below. The use of this work for commercial purposes is prohibited; its translation into other languages and adaptation/modification requires prior written permission. Questions or comments can be referred to MNE7_secretariat@apan.org.

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **08 JUL 2013**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE **MNE7 Access to the Global Commons Outcome 3 Cyber Domain Objective 3.5 Cyber Situational Awareness Concept of Employment for Cyber Situational Awareness Within the Global Commons Version 1.0 Dated 25 Feb 2013**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Nations and organisations require concepts and capabilities for anticipating, deterring, preventing, protecting against and responding to a disruption or a denial of access to the global commons domains (air, maritime, space and cyber) and for ensuring freedom of action within them, while taking into account their interrelationships.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**24**	

MULTI-NATIONAL EXPERIMENT 7 ACCESS TO THE GLOBAL COMMONS Cyber Domain Outcome 3 Objective 3.5

MNE7 Problem Statement Nations and organisations require concepts and capabilities for anticipating, deterring, preventing, protecting against and responding to a disruption or a denial of access to the global commons domains (air, maritime, space and cyber) and for ensuring freedom of action within them, while taking into account their interrelationships.

Outcome 3 Decision makers can gain sufficient understanding (including legal) and situational awareness of their own networks and relevant parts of wider cyberspace, drawing upon integrated and collaborative information, improving their ability to make timely, informed and effective decisions on the actions that allow us to anticipate, deter, prevent, protect, respond and rapidly affect an adversary's ability to disrupt or degrade our access to and freedom of action within the global commons.

Objective 3.5 Develop a framework for gaining and maintaining collaborative and integrated situational awareness.

Scope The scope of Objective 3.5 *cyber domain situational awareness* is to retain a broad concepts development and experimentation approach that encompasses international, national and military aspects, primarily focused at the strategic level, whilst recognizing the blurring of the strategic, operational and tactical levels of decision-making.

Concept of Employment A concept of employment (CONEMP) describes how a new capability will be employed and is primarily written to allow the requirements for that capability to be refined through assessment work up to a major decision point, at which the solution and expenditure are approved. The concept of employment is for a specific capability within a range of operations and scenarios; it should not presuppose any specific solution.

Situational Awareness The understanding of the operational environment in the context of a commander's or staff officer's mission or task.[1]

There is no agreed definition for global commons. For the purposes of international law it focuses on areas where no country lays claim to exclusive sovereignty and where nations have agreed to a set of permissible uses and prohibitions in its use. It is recognised that relating cyberspace to the global commons is not as simple as for the maritime, air and space domains. NATO Allied Command Transformation (ACT) Global Commons Food-For-Thought paper (March 2011[2]) to the NATO Military Committee offers the following:

In academic literature there is broad agreement that parts of the Maritime (open ocean), Air (outside of what is considered national airspace), and Space domains comprise the global commons. Cyberspace has been identified by some as a new addition to the global commons, because it shares a number of similarities. Cyberspace is not owned or controlled by any single

[1] For a more academic definition of situational awareness see M.R. Endsley, D.J. Garland, *Situational Awareness Analysis and Measurement*, Lawrence Erlbaum Associates, Hillsdale, New Jersey, USA 2000. They define Situational Awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future".

[2] http://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf

entity or sovereign state and it is potentially accessible to any and all actors with the requisite technological capabilities. The Cyberspace domain, however, is also very different from the traditional global commons. The established domains are physical, whereas cyberspace is also virtual. By definition the global commons are not owned, whereas the man-made components that comprise in their totality the infrastructure that generates cyberspace are owned, albeit by a very disparate and large group. Nevertheless, …since the cyberspace domain is of increasing importance to our security and there is a growing need for mechanisms to regulate the domain, there is logic and utility for including it under the umbrella of the global commons. Cyberspace will therefore be considered as an enabling domain that has an increasing influence on the way the other domains are accessed.

CONCEPT OF EMPLOYMENT FOR CYBER SITUATIONAL AWARENESS WITHIN THE GLOBAL COMMONS

Reference:

A. MNE7 Campaign Lexicon, draft version 0.4, dated 28 November 2011.

PART 1 - INTRODUCTION

BACKGROUND

1. The nature of cyberspace is such that it is impossible to prevent ‘new attacks’ or even predict all threats. An ‘attack’ will happen somewhere, but for those not immediately affected, capability can be maintained through the understanding of ones own vulnerabilities and building in resilience/ mitigation that can be activated through the provision of sufficient early warning[3]. The latter requires situational awareness (SA) of cyberspace.

2. There is currently a gap in the ability of our decision-makers to understand and gain sufficient SA of the cyber domain at the national and international. This reduces their ability to make timely, informed and effective decisions on the actions needed to effect an adversary’s ability to disrupt or degrade our access to and freedom of action within the global commons. Nations and organizations require the ability to use information to create sufficient, integrated, collaborative, and contextual, situation specific national and international understanding and situational awareness to support their strategic to tactical level decision-making. They must therefore collectively address the ends, ways and means to generate and sustain a national and international cyber situational awareness, of own and adversary activity, in the cyber domain.

AIM

3. The aim of this paper is to describe the concept of employment for a cyber situational awareness capability that will support international and national access to and freedom of action within the global commons.

DEFINITIONS

4. There is no coherent and agreed lexicon or taxonomy that supports cyber domain SA across governments, agencies, allies, industry and academia. Multinational Experiment 7 (MNE7) has therefore produced a Campaign Lexicon (Reference A) to enable coherent progress of MNE7 outcomes and objectives through common understanding. This concept of employment for cyber situational awareness uses the following definitions (from the Lexicon):

Cyberspace: Cyberspace is a time-dependant set of interconnected information systems and the human users that interact with these systems[4].

Situational Awareness: The human perception of the elements of the operational environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.[5]

[3] Objective 3.1

[4] Cyberspace: Definition and Implications. Rain Ottis, Peeter Lorents, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf

[5] Based on: Endsley, Mica R.: "Toward a Theory of Situation Awareness in Dynamic Systems"; Human Factors 37:1; 1995

Cyber Defence: The application of security measures to protect communication and information systems infrastructure components against cyber threats.**[6]**

5. Definition of Understanding. Understanding is defined as *the perception and interpretation of a particular situation in order to provide the context, insight and foresight required for effective decision making*[7]. It is about making better decisions based on the most accurate depiction possible.

6. Establishing Context. The term *understanding* has a number of similar, but subtly different, meanings dependent upon the context in which it is used and the user communities or institutions who develop it. For example, military understanding traditionally relates to what military forces need to understand to identify, monitor and defeat adversaries; economic understanding is based on a framework of competition, supply, demand, regulation and risk. Each context provides a different interpretation or frame of reference.

7. Insight and Foresight. Whatever the context, understanding involves the acquisition and development of knowledge to such a level that it enables insight *(knowing **why** something has happened or is happening)* and foresight *(being able to identify and anticipate what **may** happen)*[8]. Developing understanding relies first on having sufficient SA to identify the problem[9]. Analysis of the SA provides greater comprehension (insight) of the problem; applying judgment to this comprehension provides understanding of the problem (foresight). Foresight will never be perfect, but improving the quality of our information sources and the analysis of them will make it more certain.

CONTEXT

INFORMATION LAYERS AND THE CYBER DOMAIN

8. Cyberspace can be considered within the context of the six layers that contribute to the information environment (see Figure 1), sometimes simplified to three: physical, logical and social. Cyber SA is frequently focused on the bottom three of the six layer diagram (Information, network, real world) or the physical and logical - however the other layers also make a significant contribution, both directly and indirectly.

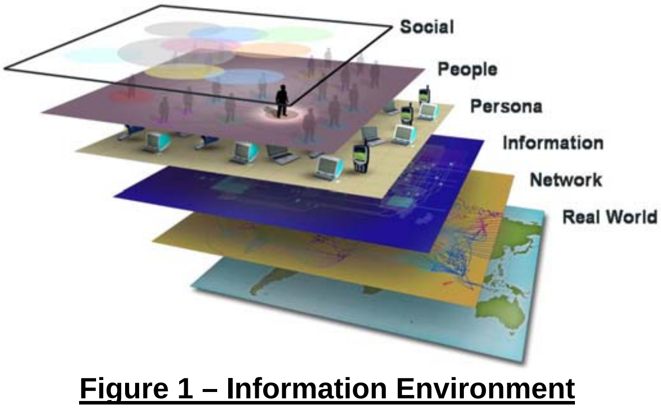


Figure 1 – Information Environment

Although convenient to visualize the 6 layers as in Figure 1, in reality the interrelationship between them is completely ad hoc and difficult to define.

[6] Based on: NATO: MC 0571 – NATO Cyber Defence Concept; 21 February 2008

[7] Concise Oxford English Dictionary (COED), 11th Edition.

[8] Insight is the capacity to gain an accurate and deep understanding of something; and foresight is the ability to anticipate future events or requirements. (COED)

[9] It should be noted that SA is the appreciation of what is happening, but not necessarily why it is happening.

9. **Physical**. The physical layer (real world and network) consists of a geographic aspect - the physical location of elements of a network, such as under the sea, or under the ground or in a building - and the physical network components, which consists of: physical hardware and infrastructure (wired, wireless and optical); and the physical connections (wires, cables, radio frequency, satellite communications, routers, servers and computers).

10. **Logical** (Virtual). The logical layer (information) comprises the logical connections that exist between network nodes. A node is any physical device connected to a computer network; for example, computers, personal digital assistants and cell phones. The logical layer includes applications, data flows (across all means) and protocols that enable interactions across the physical layer, along with the configuration of individual networks. The logical layer also includes details of: communication service providers, transfer protocols and internet domain names and ownership.

11. **Social** (Cognitive). The social layer (persona, people and social) comprises the details that connect people to cyberspace and the actual people and groups who interact by using the networks. Unique addresses or titles are matched to virtual addresses, which in turn map to the physical layer. A single person can have multiple persona; and equally, multiple people can share a single persona. The social layer can be further analysed through sub-areas such as, social networking; operating procedures; maintenance; and security.

SCOPE

12. MNE7 retains a broad scope to concepts development and experimentation on cyber SA. It recognises the all pervasive nature of cyberspace; that it underpins virtually all aspects of modern life – social, business, military, government – both good and bad, at all levels of society. However to bound MNE7, the cyber domain outcome statement includes the phrase SA of their own networks and relevant parts of wider cyberspace. This concept of employment is, therefore, focused on cyber SA required to support decision-making in the context of cyber defence.

13. The purpose of developing a concept of employment for cyber situational awareness is to provide the context for then developing a framework of processes for gaining and maintaining cyber situational awareness in relation to the global commons. This concept of employment will describe how a cyber situational awareness capability will be employed, and it is primarily written to allow the requirements for this capability to be refined by capability developers. It will not presuppose any specific solution but will consider a range of scenarios and operations.

14. The rapid pace of technological and social change, actual events and shocks in the cyber domain will require us to continually re-evaluate our understanding. This concept of employment provides an approach that addresses current understanding of the short term, out to 2015, and guidance for the longer term. There is always the risk that our assumptions and understanding of the problem statement may be challenged by actual events in this dynamic and transforming domain.

ASSUMPTIONS

15. The challenge presented by cyberspace demands a comprehensive and whole of government approach by the international community. This requires participation from public and private actors, both civilian and military, enabled by unity of effort across all instruments of national and international power.

16. Extant national and international legal frameworks (agreements, treaties and law) are fixed for the purposes of MNE7 solution and product development.

PART 2 - POLICY DRIVERS

17. States and international bodies are rapidly coming to terms with their requirements for cyber security, in this interconnected, fast-moving and uncertain world. The majority of states now possess or are developing their own national cyber security strategies and policies, as a contribution to their overarching national security strategies. These national strategies must balance the ends, ways and means, and be realistic in light of the ways and means available, as they primarily focus on ensuring security and resilience within their own states. Most states also aspire to shaping or supporting a more stable world, by promoting democratic core values (such as freedom, fairness, transparency and the rule of law) and a free and more stable cyberspace. Through these national strategies, most states are putting in place their own structures and organisations across government, industry and within their militaries. There is no single model for cyber security and cyber situational awareness in particular, and each nation has their own national interests and requirements to manage. All, however, should recognise the need to establish stronger relationships and trusted alliances with industrial partners and international counterparts.

18. As an example of one states approach, the United States has several policy documents pertaining to cyber. The Comprehensive National Cyber Security Initiative consists of a number of mutually reinforcing initiatives with major goals designed to help secure the United States in cyberspace. These goals include: establishing a front line of defence against today's immediate threats by enhancing shared situational awareness of network vulnerabilities, threats, and events, along with the ability to act quickly to reduce their current vulnerabilities and prevent intrusions; defending against the full spectrum of threats, enhancing United States counter-intelligence capabilities and increasing the security of the supply chain for key information technologies; and strengthening the future cyber security environment by expanding cyber education, coordinating and redirecting research and development efforts, and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

19. NATO policy, strategy and doctrine for cyber are less developed than that articulated in the United States. NATO has viewed the majority of cyber threats to be financially motivated and responded to as cyber crime, handled by national and international law enforcement bodies such as Interpol and Europol. NATO is concerned, and has been responding to, cyber threats with political or military motivations to exploit vulnerabilities related with cyber espionage or critical national infrastructures and online services. In 2008, nations issued a NATO policy on cyber defence which mandated NATO to protect own networks; to assist a member nation when requested; and to establish the NATO Cyber Defence Management Authority. The policy provided direction to NATO civil and military bodies and recommendations to NATO nations in order to ensure a common and coordinated approach to cyber defence and any response to cyber attacks. NATO also developed the concept of a Rapid Reaction Team on cyber defence, endorsed by nations, and resourced in 2012. More recently, NATO has agreed an updated concept on NATO's Cyber Defence (March 2011) and Cyber Defence Policy, and has developed an Action Plan (July 2011) for its implementation, which includes aspects of situational awareness capability.

20. The European Union's effort on cyber security is progressed under the Digital Agenda programme, which is one of the seven flagship initiatives of the European 2020 Strategy announced by the European Commission in March 2010. Since 2005, the European Union's technical cyber security capability has been placed with the European Network and Information Security Agency, located in Crete, Greece. This agency provides the European Union with a body of expertise to carry out very specific technical, scientific tasks in the field of Information Security. Together with the European Union institutions and the Member States, the European Network and Information Security Agency seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union. The European Commission announced two new measures to ensure that Europe can defend itself

from attacks against its key information systems. These measures are a proposal for a directive to deal with new cyber crimes and a regulation to modernise the European Network and Information Security Agency.

21. Within the United Nations, the First Committee (Disarmament and International Security) of the United Nations General Assembly addresses the policy aspects of cyber security under the auspices of information security. In 2009, the committee's national experts group, including the United States, Russia, China, France and Germany agreed on a text seeking 'development of norms for state's use of information technologies'. This agreement has been recognised by many as a breakthrough. Technical cyber security work within the United Nations is progressed under the International Telecommunications Union.

22. The International Telecommunications Union (ITU) is an agency of the United Nations which regulates information and communications technology issues. Its mission is to enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access to the emerging information society and global economy. The agency is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, convergence in fixed-mobile phone, internet access, data, voice, television broadcasting, and next-generation networks. The International Telecommunications Union membership includes 191 member states and more than 700 telecommunications sector members and associates. On the 20 March 2009 the global headquarters of the International Multilateral Partnership Against Cyber threats was inaugurated in Kuala Lumpur, Malaysia. These facilities host the ITU's Global Cyber Security Agenda, which is an international framework for cooperation aimed at finding strategic solutions to boost confidence and security in an increasingly networked information society. This was the world's first global public-private initiative against cyber threats, providing member states with expertise, facilities, real-time information, and rapid access to resources to address the threats.

PART 3 – STRATEGIC CONTEXT

THE OPERATIONAL ENVIRONMENT

THE GLOBAL COMMONS

23. The domains of international maritime waters, airspace, space and cyberspace are now integral elements of our global world. The prosperity and security of nations rely on the smooth flow of goods, information and people through these four domains – collectively known as the global commons.

24. No one nation controls access to, and freedom of action in, the global commons. The global commons do, however, form a significant element of the international security environment operating space. The global commons enable physical and virtual movement and operations for all; therefore, military, civilian, or commercial activity across the global commons is inherently interwoven and difficult to differentiate. There will also be competing perspectives that each individual state or international alliance or organization will have on activity within the global commons. Understanding the global commons is exacerbated as they extend into and connect with one another, through national territories, infrastructures, information systems and people.

25. Many nations assume, and depend upon, access to the global commons; and adversaries will challenge this. The security of globally distributed international communications paths, and therefore access to and freedom of action in the global commons, is of mutual interest and importance to nations and organisations.

SECURITY CHALLENGES

26. Against the backdrop of our access to and freedom of action in the global commons, nations and organisations face an increasingly complex set of security challenges. The period from now through to 2020 might be considered a time of transition, characterized by instability in the relation between states, and groups within states. The world now faces rapid population growth, resource scarcity, a resurgence in ideology and a contest between dictatorship and democracy. States are therefore competing for regional and global influence in the international community and global economy.

27. The rapid development in global communications has resulted in easier access to information by all. Physical dispersion is no-longer a barrier to the sharing of ideas, interests or beliefs by individuals, organisations and governments. The physical separation of cause and effect can be huge.

28. All nations and organizations are now dependent on complex networks of physical and virtual infrastructure for their resources, trade, capital and intellectual property; and their critical information and national infrastructures (communications, emergency services, government and public services, finance, energy, food, health, transport and water) now use technologies and systems that almost totally rely on access to cyberspace. These technologies and infrastructures, such as networked industrial control systems, are vulnerable to physical and virtual disruption and denial. Cyberspace is rapidly becoming the ‘common’ global common.

THE CHARACTER OF CONFLICT IN CYBERSPACE

29. In facing this increasingly complex set of security challenges, all states must also recognise that the character of conflict is constantly changing. Adversaries will continue to counter others conventional strengths, through access to cheap technology, enabling them to erode any nations

qualitative technological advantage. States cannot therefore always rely on an ability to achieve superiority in any domain. An adversary will likely use the full range of tactics available to them, such as kinetic and non-kinetic capability. They will seek to gain influence and they might incite and use proxies to conduct exploitation and offensive action on their behalf.

30. The ability to identify, understand and counter such adversaries will be difficult tasks, which must be performed on a local, regional and global scale. States will likely be engaged in conflict that could be linked across large physical distance and the operating environment will include the cyber domain.

31. Operations in cyberspace are particularly attractive given the ability to remain anonymous, making it difficult to determine the source of incidents and to discriminate between malicious acts and individual or organisational negligence. Cyberspace activity may also be a precursor to, or an indicator of, wider activity across the other global commons. As with the other domains, the operating environment can characterized as: contested, congested, cluttered, connected and constrained.

Character	**Across all Domains**	**Cyber Domain**
Contested	The ability to access, manoeuvre and influence will be fought for.	No one individual, organization or nation controls access to, and freedom of action within, cyberspace. Cyberspace in itself is no respecter of hierarchy or the level of user, indeed its freedom of use is its attraction.
Congested	People will be unavoidably drawn into urban areas, the littoral and lower airspace.	Individuals, organisations and nations have been drawn into using technologies and systems that almost totally rely on access to cyberspace. Network limitations and constraints may create the impression of congestion.
Cluttered	A mass of ambiguous targets challenge the ability to understand and discriminate.	Cyberspace enables anonymity, making it difficult to determine the source of incidents and to discriminate between malicious and individual or organisational negligence.
Connected	All activity, including that of adversaries, will rely on inter-connected networks.	Cyberspace is rapidly becoming the ‘common’ global common, with complex and adaptive networks constantly evolving on a local, regional and global scale. These networks are potentially available to anyone with access; amorphous with no obvious leader/hierarchy.
Constrained	Legal and social norms will place constraints on the conduct of operations.	There is an increasing need for common principles, understanding and norms of behaviour to be established amongst stakeholders and users to address the security issues that arise from the conduct of activity in and through cyberspace.

AN ‘ALL PERVASIVE’ THREAT

32. The range of threats and threat actors within the cyber domain is extensive, complex and difficult to understand and bound. State and non-state actors will use cyberspace for crime, espionage, subversion and sabotage, in order to attempt to gain advantage over another state or international organisation. Any infrastructure or physical asset that has any dependency on cyberspace is a potential vulnerability and dependency goes well beyond networks – of particular

concern are industrial control systems and people. Vulnerabilities residing within societies (people) are particularly worthy of note, given the huge expansion in social networking technology and activities.

33. A significant percentage of civilian and military users, at all levels, lack awareness of the vulnerabilities and threats associated with the use of cyberspace, yet dependence on cyberspace continues to increase; e.g the introduction of 'smart' metering systems, SCADA/ICS10 systems and the proliferation of mobile internet (including personal) devices.

34. Adversary structures are complex, no longer just State actors but also organised crime, hactivists (state sponsored and otherwise), emerging social groupings and some commercial (formerly called mercenary) organisations. Both state and non-state actors, including criminals and terrorists, can conduct hostile intelligence gathering, crime, disruption of critical services, and exertion of influence over people or governments, as an accessible and potentially non-attributable threat vector. These actors can operate at a safe distance with global reach, and from countries where authority is weak and/or corruption is rife. The threat posed by potential 'attackers' to networked and data systems can be determined from the attackers intent/motivation, capability and the ways and means of access[11].

35. This 'all pervasive' threat can also be considered from the perspective of four threat vectors: physical activity; influence activity; electromagnetic spectrum activity; and computer activity. These vectors, along with the corresponding protection required, are shown at Figure 2.

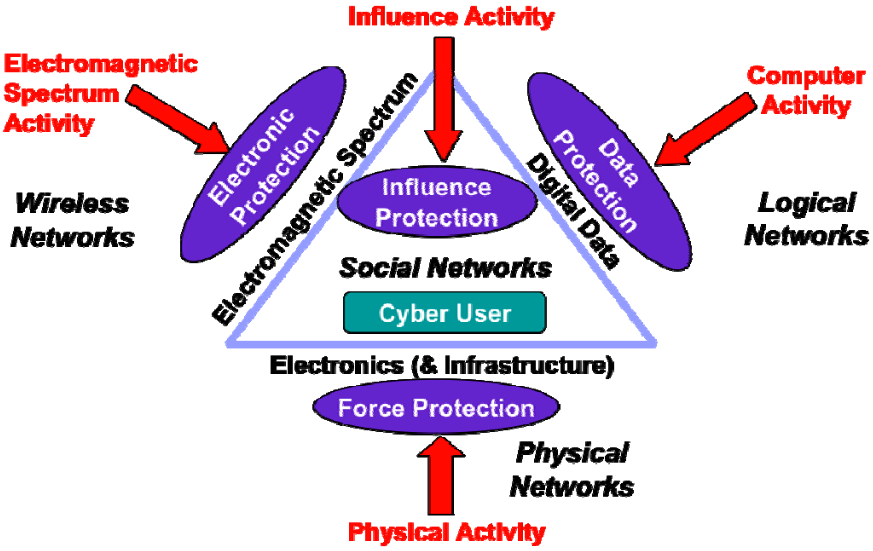


Figure 2 – Threat Vectors Against the Cyber Domain

KEY DEDUCTIONS

36. Drawing on the key themes from the security challenges and future character of conflict mentioned above, some key deductions that emerge in relation to cyber situational awareness are:

a. Decision-makers within states, coalitions and partnerships need to collaborate and contend with the intent and understanding of other commanders, national leaderships, international partners, industry, and non-government organizations, each of whose own

[10] Supervisory Control And Data Acquisition (SCADA) is a type of Industrial Control System (ICS).
[11] Objective 3.1

political, military and other aspirations will often contradict. To achieve understanding and SA of cyberspace, information needs to be drawn from the community who use it.

b. Incidents in the cyber domain can occur within seconds, and cause major disruption or denial effects on the functions of states, organisations and individuals, along with the ability to achieve rapid influence over people (adversaries, neutrals and friends)[12]. This blurs the traditional relationship between strategic, operational and tactical decision-making and therefore increases the importance of having an ability to create sufficient cyber situational awareness across the public and private sectors, and at a national and international level.

d. The different threat vectors means that nations and organisations need to understand more than just technical aspects of cyberspace; for example, they must also detect, analyze and assess societal and human interactions, behaviours and intentions. An adversary will likely use a full range of tactics, techniques and procedures, such as kinetic and non-kinetic capability; they will contest to gain influence and they will incite and use proxies to conduct actions on their behalf.

e. Cyber situational awareness must be considered in a holistic fashion, in context, along with situational awareness generated in the environments of Maritime, Land, Air and Space, and Electromagnetic. The interdependence of these domains is complex, the boundaries, if applicable, indistinct, and activities within each overlap. However the provision of cyber SA may enable the identification in the cyber domain of potential threats before they manifest themselves in the more physical domains.

[12] See Pat Muoio's econometrics slides at: http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2010-11/Muoio_P_themes-ISPAB.pdf

PART 4 – CAPABILITY DESCRIPTION

ROLE

37. Having an ability to create a national and international picture of what is happening in cyberspace across the public and private sectors will be important if we are to provide a comprehensive response to sophisticated threats. These threats could be operating below the detection thresholds of many existing systems, and may seek to disrupt or deny partners and coalition members access to cyberspace. Generating and sustaining national and international understanding and situational awareness of the cyber domain is, however, a complex problem. It must be met collaboratively by all stakeholders to truly provide a comprehensive and integrated response to the sophisticated cyber threats that challenge our access to and freedom of action within the global commons. This requires: improved methodologies for threat, vulnerability, risk and dependency assessment; collaborative information sharing; clear legal analysis; appropriate use of enabling technologies; and a framework of processes that deliver cyber situational awareness. All of this must be done collaboratively across public and private sectors, at a national and international level.

FUNCTIONS

38. A sub-national, national and international information sharing framework for providing 'global' SA of own and adversary activity, across public and private sectors, is required to mitigate abnormal cyber events through the provision of timely and effective warnings. This could then be used to support a comprehensive response to threats. Such a capability must encompass the use of cyberspace at all levels and at any scale, to underpin decision-making processes from the strategic to tactical level of operations. As the threat and severity of impact escalates, the cyber SA picture presented will require appropriate degrees of timeliness, richness, and accuracy; equally, what is presented and how, must be appropriate to the level of decision maker.

39. A cyber SA capability will require the functions of Detect, Assess and Inform. However these require the underpinning capability to establish and monitor baseline conditions, recognise and conduct diagnosis of anomalies, visualise data to support mitigation strategies and where appropriate enable attribution to be established.

40. Part of establishing the baseline state of cyberspace is gaining visibility of/ assurance of, the status of participating actors in regard to implementation of current protection measures.

DETECT FUNCTION

41. The Detect function will primarily generate a degree of perception. This is the ability to detect anomalous activity in respect of a recognised baseline (normal activity); by collating the information received from multiple sources both within and outside an organisation/community of interest. Perception provides basic information about the attributes and dynamics of relevant elements within cyberspace; this then yields the basic building blocks for comprehension and prediction.

42. Gaining and maintaining cyber SA will require the management of large volumes of structured and unstructured data from a wide range of sources. In addition to detecting and analysing 'immediate' anomalies there is also the need to identify longer term anomalous activity, or trends, based on continuous comparison with previous (historical) data. Such processes will be highly dependent on automated technologies that collect, securely store and monitor related events and patterns.

ASSESS FUNCTION[13].

43. The Assess function will primarily generate a degree of comprehension. Comprehension encompasses how people combine, interpret, store, retain and retrieve information and includes the integration of multiple pieces of information and a determination of their relevance to a decision-maker's goal. The assess function here is dependent on understanding ones' own dependency on cyberspace and being able to match it to the identified anomalous activity. If it matches it poses a potential threat. The ability to assess the impact and risks posed to the systems and services can be identified through a criticality, dependency and vulnerability analysis[14].

44. The Assess function requires cyber SA to be placed in context. The fusion of data from many sources (including historical) and all domains to generate a composite SA picture will enable the identification of patterns and broader, co-ordinated activities/threats.

45. Comprehension will require the fusing of data into appropriate levels of abstraction. Assuming that data is rich in context, it will have to be filtered and then correlated to provide a visualisation that is appropriate to the level at which it is to be used. Flexibility in the processing of data will be required to allow for the possibility of errors; data obtained that initially appears unintelligible should be retained for subsequent further analysis. It is also important to understand the human element - that creating a recognised or common 'picture' involves not just a degree of filtering, but that an operator brings with him his own experience and imagination in interpreting the 'picture'.

46. The Assess function will also generate a degree of prediction, which involves the ability to use the knowledge of the status and dynamics of the situation, combined with any criticality, dependency and vulnerability analysis, to make projections into the future. Prediction will require the interpretation, distribution and archiving of the information visualised. At present there are a lack of suitable models that can replicate cyberspace, however prediction techniques are evolving; the application of 'foresight' techniques, such as horizon scanning, will aid prediction and possible mitigation of 2nd and 3rd order effects. Gaming technologies may be exploited to anticipate most likely future outcomes.

47. Underlying the assess function is trust - the degree of assurance and integrity of the initial data gathered through detection. A number of techniques such as authentication, protocols, and 'signature' management exist but the imposition of such techniques must be balanced against the perceived benefits to stakeholders[15]. In considering any follow up action requiring legal support, the legal requirements will drive the level of trust and confidence to be achieved.

INFORM FUNCTION

48. The Inform function is the ability to share information collected with those who require it, in an easily digestible format – it will require rapid and trusted information exchange with a wide range of sources. Critical to a cyber SA capability will be data processing and management as will the ability to fuse cyber SA output with other 'intelligence' outputs to create a 'global' SA picture. Given the expected volume of data this will only be practicable with a degree of automation and will also require item tagging (e.g. metadata) and true Multi-Level Security (MLS) particularly to ensure effective presentation /visualisation.

[13] Objectives 3.1,3.3, 3.4

[14] Objective 3.1

[15] Objective 3.2

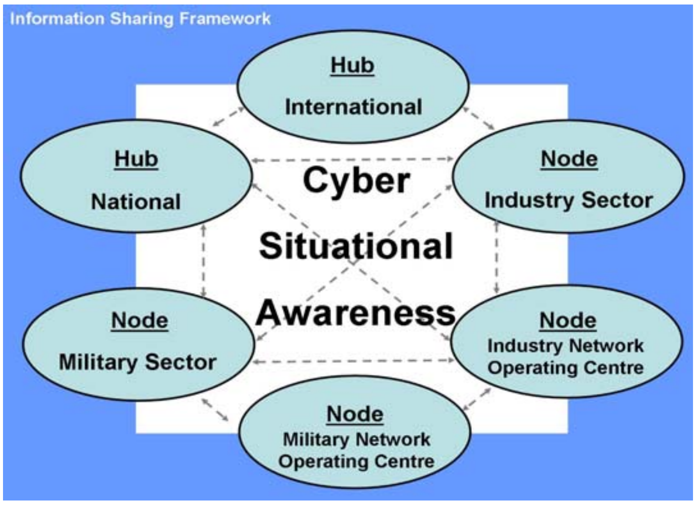


Figure 3 – Information Sharing Framework

49. The data needs to be effectively communicated to decision-makers in a manner that provides them with information of appropriate detail and quality, in a timely manner. These attributes will have to be balanced against the desire to reduce the barriers to participation and facilitate its rapid dissemination. Information produced should ideally be at as low a security classification as possible and across all operating levels - across a sub-national, national and international integrated information sharing framework (see Figure 3).

50. Other limitations/restrictions on the flow of information, such as transfer protocols, regulation, legislation and treaties, should be kept to a minimum and only where deemed essential, understood/justified and mitigated. Organisation which process sensitive and information face conflicting pressures to keep this data secure and yet allow access by authorised users. Participation in the sharing network should be voluntary and it is recognised this will require unprecedented degrees of trust e.g. commercial intellectual property rights (IPR).

PROCESS

51. Cyber SA is the understanding of anomalies identified, individually and when aggregated, in relation to ‘normal’ activity in cyberspace in the context of a mission or task. The Detect and Assess functions within a cyber SA capability comprise activities that deliver perception; comprehension; and prediction. Perception, comprehension and prediction will promote a parallel process, with continuous updates provided to and from each element that are presented to the decision-maker.

52. As with any SA, SA of Cyberspace can be related to Boyd’s Observe, Orientate, Decide, Action (OODA) loop. Cyber SA will contribute to the ‘observe’ and ‘orientate’ elements, enabling the decision-making (decide) to go ahead (see Figure 4). The current difficulty is in ascertaining a confidence level for the information gleaned from cyberspace given it is a relatively new domain and not yet fully understood.

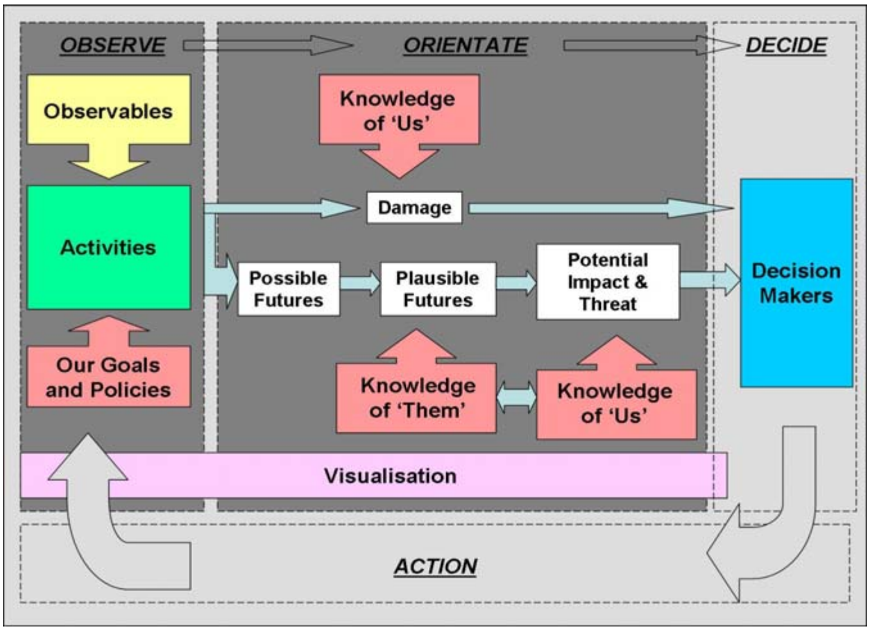


Figure 4 – Situational Awareness Process Model[16]

53. Cyber SA capability will contain processes and components that incorporate: improved methodologies for threat, criticality, dependency, vulnerability, risk and resilience assessment[17]; collaborative information sharing[18] clear legal analysis[19] appropriate use of enabling technologies[20]; and a framework of processes that deliver cyber SA[21]. A cyber SA capability would benefit from automated computer applications with varying degrees of human intervention. However there remain other important processes to consider, among which are:

a. The relationships and partnerships required across stakeholders, and cultural aspects / differences;

b. Assessment of capability accuracy and confidence, and how to handle uncertainty;

c. Ownership, responsibilities, spheres of action, provision of resource and effort;

d. Simulation capability requirements for training, 'what if' analysis and mission rehearsal;

e. Monitoring innovation both within cyberspace and how people chose to use it.

CYBER DOMAIN CONSTRUCTS

54. Cyberspace can appear to lack any easily defined boundaries and there can be interaction with cyberspace across any one, or more, of the 6 Layers shown in Figure 1. There is always the potential for an actor beyond any (arbitrarily) defined cyber boundary to carry out a malicious act that has an affect throughout cyberspace. The issue of defining a boundary is likely to be driven by that over which one has control and/or the amount of data that can be effectively handled - a cyber SA capability will require the coordination, aggregation and fusing of cyber information from both the public and private sectors and across both national and international boundaries. Some

[16] Ibid.

[17] Objective 3.1
[18] Objective 3.2
[19] Objective 3.3
[20] Objective 3.4
[21] Objective 3.5

boundary definitions (categorisations) do exist already; two constructs currently used to describe cyberspace – open and closed networks; near, mid and far operating spaces are discussed below. These constructs can be used to describe what degree of cyber SA capability is required, or possible.

OPEN AND CLOSED NETWORKS

55. Network architectures may be permanently connected (open) or permanently disconnected (closed) to other networks. Closed networks are rarely totally isolated; they may have to link to wider networks or be accessed by personnel, with varying frequency for activities such as maintenance, system updates, or to retrieve and forward data. The critical weakness is the seam between open and closed networks. Open networks will face (be open to) the complete range of threats and vulnerabilities and sufficient SA is required to ensure associated risks are understood and any mitigation (resilience) measures, in place and appropriate. To obtain such cyber SA, information will need to be drawn from both types of network – open and closed.

NEAR, MID AND FAR OPERATING SPACES

56. Cyberspace can be considered through the construct of interconnected near, mid and far operating spaces. This construct has sub-national, national and international utility across the strategic to tactical level. Perspectives of near, mid and far operating spaces will differ depending on each nation, organisation or person's situation, span of command and responsibility. The critical points are the seams between near, mid and far operating spaces.

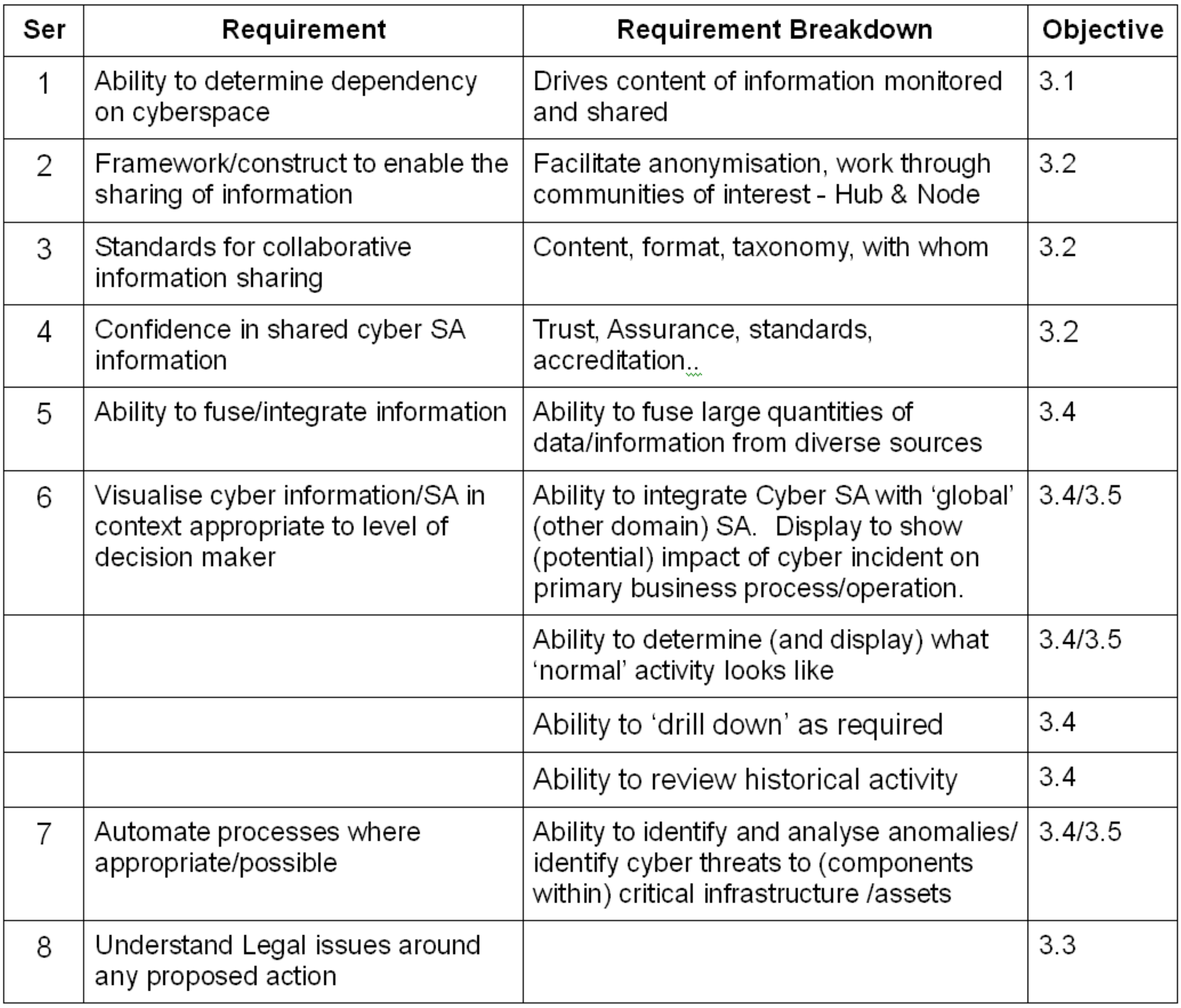
57. Near. The near operating space contains those networks and systems that are critical to operations that nations and organisations must protect. It might comprise national computer and telecommunications systems owned and assured by government. The near would include military networks, such as information infrastructures and mission planning systems. The near will also include aspects of a nation's Critical National Infrastructure and Information. The near operating space could include a nation's Defence Industrial Base, key allies, and companies deemed to be of national strategic importance.

58. Mid. The mid operating space contains networks and systems that are critical to operations, but which the government or military do not protect themselves. It might comprise major infrastructure providers across a nation, such as utilities companies, telecommunications providers, virus scanning companies, cryptographic companies, and satellite service providers. Nations and organisations depend upon networks and systems in the mid to connect their distributed hubs of activity in the near operating space. Nations and organisations must have sufficient SA of the mid operating space, to give confidence in the availability and protection of their own activity.

59. Far. The far operating space contains those networks and systems that, if influenced, will prove critical to operations. It comprises those networks and systems where protection, access, exploitation, and use is not assured. The far might include social networking sites, news media sites, and offshore information technology and data repository services provided over the internet. Nations and organisations will have many suppliers and contractors who store data and utilise applications on systems that reside in the far operating space.

REQUIREMENTS

60. The initial, high level, requirements for a cyber SA capability are shown below:



Ser	Requirement	Requirement Breakdown	Objective
1	Ability to determine dependency on cyberspace	Drives content of information monitored and shared	3.1
2	Framework/construct to enable the sharing of information	Facilitate anonymisation, work through communities of interest - Hub & Node	3.2
3	Standards for collaborative information sharing	Content, format, taxonomy, with whom	3.2
4	Confidence in shared cyber SA information	Trust, Assurance, standards, accreditation..	3.2
5	Ability to fuse/integrate information	Ability to fuse large quantities of data/information from diverse sources	3.4
6	Visualise cyber information/SA in context appropriate to level of decision maker	Ability to integrate Cyber SA with ‘global’ (other domain) SA. Display to show (potential) impact of cyber incident on primary business process/operation.	3.4/3.5
		Ability to determine (and display) what ‘normal’ activity looks like	3.4/3.5
		Ability to ‘drill down’ as required	3.4
		Ability to review historical activity	3.4
7	Automate processes where appropriate/possible	Ability to identify and analyse anomalies/ identify cyber threats to (components within) critical infrastructure /assets	3.4/3.5
8	Understand Legal issues around any proposed action		3.3

OPERATIONAL EMPLOYMENT

COMMAND AND CONTROL

61. Decision-makers can utilise cyber activity to gain advantage within a situation in time and space, and to generate freedom of action. Cyber activity can exploit surprise through speed, reach and potentially covert and non-attributable action. This can paralyse or disrupt an adversary’s decision-making and undermine their cohesion and trust. An effective cyber SA capability will show the ‘health’ of cyberspace, giving confidence in the availability of those activities that are dependant on it as well as providing additional SA gleaned from the aggregation of information obtained from cyberspace. It is essential that a decision maker has both cyber SA and understands his dependency on cyberspace[22].

[22] Objective 3.1

INTELLIGENCE (CYBER CONTRIBUTION TO GLOBAL COMMON OPERATING PICTURE)

62. Intelligence gathering is also dependant on cyberspace. Cyber SA provides confidence in the health of cyberspace (its status) as well as contributing to the intelligence picture in its own right through the analysis of events/anomalies detected. This may be indicative of hostile activity in other domains ranging from organised crime, through to terrorism, to national/industrial espionage. Cyber SA should be fused with information from the other domains to obtain a richer overall intelligence picture (see Figure 5).

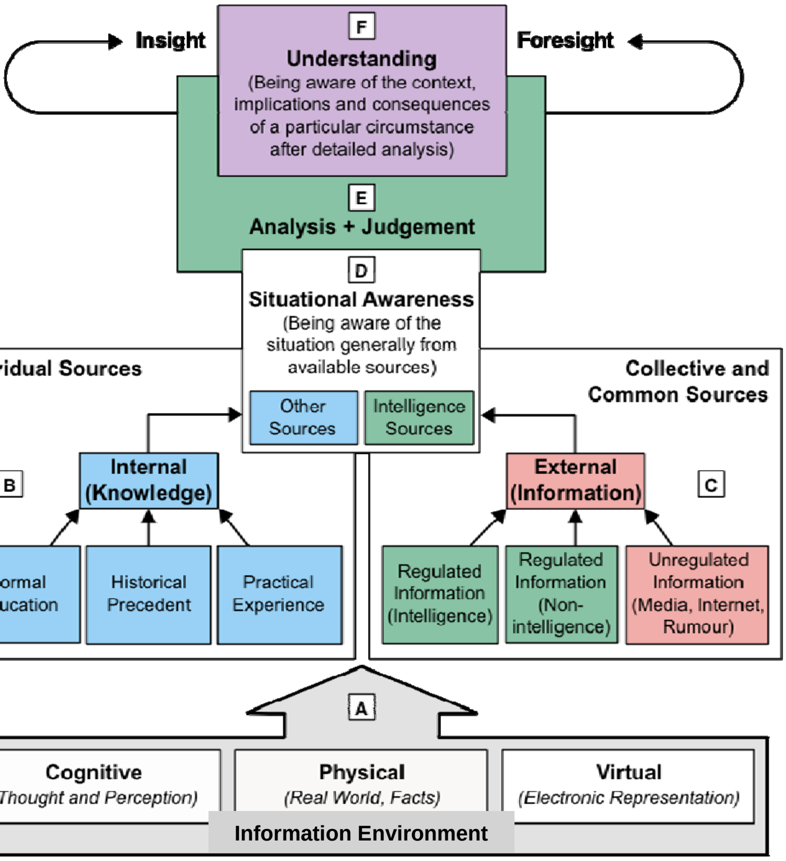

Insight
F
Understanding
(Being aware of the context, implications and consequences of a particular circumstance after detailed analysis)
Foresight
E
Analysis + Judgement
D
Situational Awareness
(Being aware of the situation generally from available sources)
Other Sources
Intelligence Sources
Individual Sources
Collective and Common Sources
B
Internal (Knowledge)
External (Information)
C
Formal Education
Historical Precedent
Practical Experience
Regulated Information (Intelligence)
Regulated Information (Non-intelligence)
Unregulated Information (Media, Internet, Rumour)
A
Cognitive
(Thought and Perception)
Physical
(Real World, Facts)
Virtual
(Electronic Representation)
Information Environment

Figure 5 – Sources of Information

INFORMATION SHARING

63. Cyber SA requires the fusion of information from as many, diverse users of cyberspace as possible in order to provide timely warnings. Ideally that information should be assured - from appropriately accredited partners, coalition members, other government departments, agencies and industry.

64. The sharing of information must be on a mutual benefit basis to ensure maximum (willing) participation, and enable stakeholder concerns to be resolved. Information confidentially and integrity must be balanced with accessibility and security along with the ability to anonymise the source; information risk management at the national and international level is pivotal. The level of security /protection afforded to this information should be appropriate bearing in mind the information pertains to awareness of activity/incidents in cyberspace and not mission/business operational data.

65. Whilst collecting information from the widest spread of sources is desirable, the quantity collected must be matched by the ability to process and act on it.

PART 5 – IMPLICATIONS FOR DELIVERING CYBER SITUATIONAL AWARENESS

TRAINING

66. The capability to achieve understanding and cyber situational awareness requires that we understand more than just technical aspects of cyberspace; it requires, for example, the ability detect, analyse and assess societal and human interactions and behaviours, including associating virtual persona created in cyberspace with real people, identifying their real relationships and intentions. This requires competence in technical and social network analysis and language skills, much of which will need to be sourced from outside the military sector.

67. For experimentation and exercise purposes, cyberspace modeling tools will need to bridge the gap between cyberspace test and evaluation tools and techniques and those modeling tools which focus more on political, military, economic, social, infrastructure and information environments. Analysis and exercise environments need to span the extent of any business or operational process layers, through network layers and into the physical domain. This will enable users to build complex multi-level network architectures, across which cyber situational awareness and decision-making can then be placed at the centre of the experimentation and exercise process.

EQUIPMENT

68. Enabling technologies provide the ability to present and portray information, activities and data in a manner that supports human analysts and decision-makers. Incidents in the cyber domain may occur in a matter of seconds, possibly having major detrimental effects on the functionality of the targets, yet humans remain essential for both assessment and decision-making activities.

69. Tools capable of managing large quantities of data and information from diverse interconnected networks in accordance with the requirements. Ultimately, analysts and decision-makers need to make sense of the information presented to them – to sufficiently understand the meaning to predict what will happen with enough confidence to take appropriate action.

70. SA is only achieved when the information gleaned from cyberspace is placed in the relevant national/organisational, real world context – this will require appropriate visualization technology.

71. The majority of cyber infrastructures are owned/provided by the private sector; any tools/technology will need to support the sharing of information across all levels of government and throughout the private sector. All information sharing participants must be able to access, retrieve, process and disseminate information relating to cyber SA.

72. Cyberspace technology, and the way in which it is used, are both evolving rapidly, and in the case of it's use, not always predictably. Technologies to generate cyber SA are currently immature but will need to be sufficiently flexible to cope.

INFORMATION

73. To achieve effective SA internationally will require nations and organisations to readily share information. Many governments have already made progress in aggregating information relating to cyber activity from the intelligence, law enforcement and military communities. The challenge remains to expand this sharing to the private sector and international partners. As information

sharing to generate the cyber SA capability expands (numerically and geospatially) so the resultant decision making (for those not directly affected by an incident) will progress from being reactive to proactive. Governments and partners should collaborate, coordinate and integrate cyber related information and analysis at the national and international level.

74. The scope of analysis – what is to be analysed – varies from one situation to another, but its purpose is always the same: to enable the decision-maker to understand the situation and to frame the problem. Generally analysis comprises an orientation to the circumstances and surroundings of a particular crisis or situation, from both a current and historical perspective, and an examination of the potential sources of conflict – the same approach should be taken in cyberspace. This will entail the management of large quantities of information from a wide variety of sources with appropriate controls to ensure accuracy, validity, currency and provenance.

75. The type of information to be collected and shared will be driven by the analysis community and will include more than that related specifically to the technical aspects of networks. It will be guided by information from many non-cyber sources and may include: assessment of adversary intent; information about incidents and attacks; and other reference information, as well as the output from threat and vulnerability assessments.

76. Intelligence and information architectures should therefore be designed to accommodate analysis, and these will likely include the following:

a. Information storage (variable formats) and archiving.

b. Continuous updating.

c. Wide but regulated access.

d. Search and retrieval (including capacity for data tagging).

e. An ability to handle large data sets that form the basis of situational awareness.

77. The effective sharing of information will be based on mutual trust and overcoming the inevitable frictions that will exist initially between nations and organisations. Within the private sector there will have to be a perceived benefit in sharing, which must outweigh any costs to participating such as those resulting from security over-classification, legislation and imposed infrastructure requirements.

78. The types of information required to be shared will include more than that just related specifically to the technical aspects of networks. Information will include: assessment of adversary intent; information about incidents and attacks; and other reference information, such as known vulnerabilities, software and hardware products, malicious software, and evaluations and certifications of products. This type of information is common to the majority of networks and, as such, should be collectively maintained by nations.

DOCTRINE, CONCEPTS & LEGAL

79. Nations and organisations are developing their cyber policies, strategies, concepts and doctrine; however, these are at varying levels of maturity, and not all are available at the unclassified level. Nations and organisations should, through their cyber strategies, address approaches by which they will develop SA of the cyber domain. To aid this, nations and organisations need to better understand and define where the boundaries and responsibilities for cyber SA reside. At present, a lack of clearly defined roles and responsibilities and a fragmented approach to information sharing is hindering development of collaborative cyber SA. Nations

would benefit from cyber doctrine at the national and international level; the cyber domain requires a comprehensive, whole of government approach, both at the national and international level, across governments, alliances, militaries, multi-agencies and industry partners.

80. Nations and organisations actions must comply with national and international laws. The applicable laws depend on circumstance, for example, the nature and location of the operations, who is conducting them, who they are conducted against, and whether or not they are conducted as part of an armed conflict. There is a requirement to raise the awareness amongst decision-makers about the legal issues related to the cyber domain and cyber incident handling, and to provide legal clarity on any proposed courses of action.

81. Practical use should be made of the legal and non-legal instruments that are already there for managing cyber incidents. Trends emerging from dealing with international cyber incidents should be combined with the comprehensive approach to international security and crisis management. An interdisciplinary approach (legal experts and cyber experts) to the legal and practical aspects of cyber security in the global commons is required.

82. There is currently a disparity between law in action and law in theory. There is a need to engage in debate across the principles and practices of different legal areas such as: law of telecommunications, network and information security, criminal law, national security law, and law of armed conflict. The challenges posed by norms of behaviour and legal frameworks would benefit from the following:

a. Raised awareness about legal issues of cyber security and ways to overcome them;

b. Increased cooperation and coordination between areas of the law as well as law and other expert areas related to managing cyber incidents;

c. Better understanding of the quality of law relevant to managing cyber incidents; and

d. Well-grounded proposals for additional legislation on an international level.

83. Greater understanding is also required of the unresolved areas within legal assessment thresholds. Decision-makers need guidelines on how to differentiate between various cyber incidents, for example, crime, terrorism, and war, to determine the legal judgment and response. There is also a need to better understand how concepts like sovereignty, *jurisdiction over* and *ownership of information infrastructure* can support national and international cyber SA and security. From a global commons perspective, there is a need to understand and consider what analogies and exceptions apply in regard to already established commons.

ORGANISATION

84. Activity within the cyber domain occurs across military, government, national and international seams; this, therefore, demands a comprehensive approach to cyber activity in support of all operations. This approach must balance the tension between interoperability and managing security. Trusted information sharing frameworks and environments are required to enable partners to each provide their valuable information and derive and shared cyber situational awareness. This will necessitate developing processes capable of identifying domain specific activities and also processes capable of identifying activities that cross other domains, such as maritime, land, air and space. These processes depend on the context of an environment and on the goals and interests of the decision-maker.

85. Situational awareness is essential for decision makers to effectively manage their resources. In a complex domain, such as cyberspace, situational awareness can greatly improve the timeliness and effectiveness of decision-making. It must, however, be recognised that cyberspace is permanently active, and that the complexity and pace of operations in cyberspace may rarely allow for the complete cognitive process to take place before a decision needs to be made. Any cyber situational awareness framework must, therefore, enable continuously evolving freedoms and constraints, which themselves reside within the strategies and doctrine set out and mandated by nations, organisations and alliances as a means to deliver their policies, procedures, standards, authorities, regulations and agreements.

INFRASTRUCTURE

86. The challenge in the cyber domain is to maintain SA over a vast number of network objects, events and individuals and groups engaged in cyber activity, in near-real-time. This requires knowing the level of threat and the current status and topography of those infrastructures, assets and capabilities, irrespective of who owns them, that are critical to operations.

87. The challenge can then be managed by understanding the dependence of those critical operational processes/assets on cyberspace and focusing resources in those areas.

PART 6 - CONCLUSION

88. There is currently a gap in our ability to generate sufficient collaborative national and international situational awareness across the cyber domain. This generates a requirement for a generic and comprehensive framework that details the processes for generating sufficient collaborative national and international cyber situational awareness. Cyber situational awareness is required across the public and private sectors, and at a national and international level, if we are to truly provide a comprehensive and integrated response to sophisticated threats that can operate below the detection thresholds of many existing processes and systems.

89. In an increasingly complex world, the relationship between strategic, operational and tactical decision making has become blurred, thus increasing the importance of having an ability to create sufficient national and international cyber situational awareness. Cyber situational awareness must also be considered in a holistic fashion, along with situational awareness generated in the physical, cognitive and virtual domains, and the environments of Maritime, Land, Air and Space, and Electromagnetic. The interdependence of these domains and environments is complex, the boundaries porous, and the activities within each are converging.

90. Ultimately, there is a requirement to understand the aggregation of the priority threats, vulnerabilities and dependencies that nations and organisations have across all domains and environments. It is these vulnerabilities and dependencies that adversaries will exploit to disrupt or deny nations and organisations access to and freedom of action in the global commons. Achieving cyber situational awareness is therefore essential if decision-makers are to effectively manage their resources. In such a complex domain as cyberspace, cyber situational awareness can greatly improve the timeliness and effectiveness of decision-making. It must, however, be recognized that cyberspace is permanently active, and that the complexity and pace of operations in the cyber domain may rarely allow for the complete cognitive process to take place before a decision needs to be made.

91. Cyberspace in itself is no respecter of physical boundaries, hierarchy or the level of user, indeed its freedom of use is its main attraction. Nations and international bodies are rapidly developing their cyber capabilities to maximise the benefits that accrue in a safe and secure manner. Many now have national cyber strategies that focus on ensuring security and resilience within their own nations. However the pace of innovation and change in cyberspace makes it almost impossible to fully understand this domain and the resultant risks associated with being at the leading edge. Issues such as the ease of achieving anonymity, combined with the low barriers to entry, make cyberspace a very attractive (and profitable) domain in which to operate for a significant percentage of the population - both good and bad.

92. The nature of cyberspace is such that it is impossible to prevent ‘new attacks’ or even predict all threats. An ‘attack’ will happen to someone/something, but capability can be maintained through the understanding of ones own vulnerabilities and building in resilience/ mitigation that can be activated through the provision of sufficient early warning[23]. The latter requires situational awareness (SA) of cyberspace.

[23] Objective 3.1